REMARKS

This application has been reviewed in light of the Office Action dated September 20, 2007. Claims 1-9, 11-14, and 16-29 are presented for examination, of which Claims 1, 13, 17, and 29 are independent in form. Claims 10, 15, and 26 have been cancelled, without prejudice or disclaimer of subject matter, and will not be mentioned further. Claims 1, 3, 11, 13, 16, 17, 19, 27, and 29 have been amended. Favorable reconsideration is requested.

The Office Action states that Claims 1-29 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0154913 (*Barriga et al.*), in view of U.S. Patent No. 5,604,803 (*Aziz*). Applicants submit that independent Claims 1, 13, 17, and 29, together with the claims dependent therefrom, are patentably distinct from the cited prior art for at least the following reasons.

The aspect of the present invention set forth in Claim 1 is directed to a method for facilitating a single access to an access provider for a user. The method includes identifying at least one primary account for the user; generating a single use user identification that is configured to be usable to gain access to the access provider; associating the single use user identification with the at least one primary account for the user; issuing the single use user identification to the user; receiving a request for authentication of the single use user identification from an access provider; determining a primary account number corresponding to the single use user identification; returning an approval message to the access provider if an account associated with the primary account number is valid; and declining the authentication request if either no primary account

number corresponding to the single use user identification can be found, or if an account associated with the primary account number is invalid.

Important features of the method of Claim 1 include the steps of receiving a request for authentication of the single use user identification from an access provider; determining a primary account number corresponding to the single use user identification; returning an approval message to the access provider if an account associated with the primary account number is valid; and declining the authentication request if either no primary account number corresponding to the single use user identification can be found, or if an account associated with the primary account number is invalid. By virtue of these features, a user is provided with single use access to a service provider, without having to create an account with the service provider, if an access verifier determines that a primary account number associated with the single use user identification is valid.

Barriga et al. relates to an apparatus and method for providing single sign-on services to a user when accessing a selected service provider from a plurality of service providers. Apparently, *Barriga et al.* teaches in FIG. 2 that a single sign-on access provider provides a token to a user. The user provides the token to a service provider. The service provider issues to the access provider an authentication query, which includes a name of the service provider and a reference to the user. The access provider responds by providing a temporary alias identity ALIAS_ID to the service provider. The service provider requests a local identity SP_ID and password from the user. The service provider requests that the access provider link the alias identity ALIAS_ID, the local identity SP_ID, and the name of the service provider. If a profile associated with the user permits such an update, the access provider authorizes the service provider to update a local

database with a link between the alias identity ALIAS_ID and the local identity SP_ID. The user is then granted access to the service provider, and greeted with the user with the user's local identity SP_ID and account.

Nothing has been found in *Barriga et al.* that is believed to teach or suggest "receiving a request for authentication of said single use user identification from an access provider; determining a primary account number corresponding to said single use user identification; returning an approval message to said access provider if an account associated with said primary account number is valid; and declining said authentication request if either no primary account number corresponding to said single use user identification can be found, or if an account associated with said primary account number is invalid," as claimed in Claim 1.

Aziz is directed to a method and apparatus for secure remote authentication in a public network. Apparently, *Aziz* teaches that a user provides a login address as a password during an anonymous file transfer protocol request. A destination server compares the user's e-mail address to a list of authorized users' addresses. If the user's e-mail address is located in the list, the destination server generates and encrypts a random number. The encrypted random number functions as one-time password for the user.

Nothing has been found in *Aziz* that is believed to teach or suggest "receiving a request for authentication of said single use user identification from an access provider; determining a primary account number corresponding to said single use user identification; returning an approval message to said access provider if an account associated with said primary account number is valid; and declining said authentication request if either no primary account number corresponding to said single use user

identification can be found, or if an account associated with said primary account number is invalid," as claimed in Claim 1.

Applicants submit that a combination of *Barriga et al.* and *Aziz*, assuming such combination would even be permissible, would fail to teach or suggest receiving a request for authentication of said single use user identification from an access provider; determining a primary account number corresponding to said single use user identification; returning an approval message to said access provider if an account associated with said primary account number is valid; and declining said authentication request if either no primary account number corresponding to said single use user identification can be found, or if an account associated with said primary account number is invalid.

Accordingly, Applicants submit that Claim 1 is patentable over the cited art, and respectfully request withdrawal of the rejection under 35 U.S.C. § 103(a).

Independent Claims 13, 17, and 29 include features similar to the ones discussed above. Therefore, those claims also are believed to be patentable for at least the reasons discussed above. The other rejected claims in this application depend from one or another of the independent Claims 13, 17, and 29 and therefore are submitted to be patentable for at least the same reasons. Because each dependent claim also is deemed to define an additional aspect of the invention, individual reconsideration of the patentability of each claim on its own merits is respectfully requested.

No petition to extend the time for response to the Office Action is deemed necessary for this Amendment. If, however, such a petition is required to make this Amendment timely filed, then this paper should be considered such a petition and the

Commissioner is authorized to charge the requisite petition fee to Deposit Account 06-1205.

In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

/Jonathan Berschadsky/
Jonathan Berschadsky
Attorney for Applicants
Registration No. 46,551

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

FCHS_WS 1627339_2